

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

18 APR 16 PM 3:07

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 APPLE IPHONE, MODEL A1661, CURRENTLY IN THE
 POSSESSION OF HSI

Case No.

1:18MJ-252

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
 See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):
 See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):


- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. Sections 2251, 2252A	Production and possession of child pornography

The application is based on these facts:

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature

Special Agent Jason Kearns, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 4/16/18

City and state: Cincinnati, Ohio


 Judge's signature

Hon. Karen L. Litkovitz, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
APPLE IPHONE, MODEL A1661,
CURRENTLY IN THE POSSESSION OF
HSI

Case No. 1:18-MJ-00252

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, JASON G. KEARNS, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent of Homeland Security Investigations (“HSI”), United States Department of Homeland Security, am hereinafter referred to as Affiant. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—one electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.
2. I am an employee of HSI assigned to the Cincinnati Resident Office. I have been employed with HSI since September 2005. I attended and graduated from the basic agent training course in Brunswick, Georgia. I have received extensive training in the investigation criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A from HSI, as well as ongoing in-service training. I have received training in the areas of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

3. This affidavit seeks the issuance of a search warrant. There is probable cause that MARK BROOKBANK violated Title 18, United States Code, Sections 2251(a) (production of a visual depiction involving the use of a minor engaging in sexually explicit conduct), and 2252(a)(4)(B) (possession of child pornography). There is probable cause to believe that evidence of these violations are contained within the Device as further described in Attachment A.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit comes from my personal knowledge and facts told to me by other law enforcement officers.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is an Apple iPhone cellular phone, marked Model A1661, FCC ID # BCG-E3087A, IC: 579C-E3087A; (the "Device"). The Device is currently located and held by HSI at the HSI Cincinnati office located at 9875 Redhill Drive, Blue Ash, Ohio 45242.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. I have communicated with the HSI Cyber Crimes Center Child Exploitations Investigations Unit ("CEIU"), and from that communication, I learned, among other things, the following:

a. On or about December 18, 2017, CEIU received an investigative lead from the Queensland Police Service. The Queensland Police Service had identified a user on a foreign

image hosting website (the “User”). The User, who registered his account on or about November 20, 2017, posted 23 photo albums on the foreign image-hosting website. The photographs that could be seen by law enforcement showed women and girls in various states of undress. Some of the photo albums were password protected.

b. One of the User’s albums, entitled “Toy,” had approximately 38 images of a girl approximately five years old. In the images, the girl was sitting in the lap of an adult male. In several of the pictures, the adult male had his hand on the girl’s butt or in her genital region. In several of the pictures, the girl was wearing only panties.

c. Queensland Police Service extracted GPS information from the photographs in the Toy album. That information came back to a specific address on Stewart Avenue in Cincinnati, Ohio (the “Cincinnati Address”). Queensland Police Service also determined that the photographs were taken with an Apple iPhone 7 Plus.

d. On or about December 20, 2017, Queensland Police Service provided information that the email address associated with the User’s account was “Lovelittleones4@gmail.com”. The IP address used to log into the email account resolved back to Cincinnati Bell.

8. On or about December 21, 2017, I and other HSI agents went to the Cincinnati Address. We spoke to an adult male resident of the Cincinnati Address (“Individual-1”) and an adult female resident of the Cincinnati Address (“Individual-2”). We identified a six-year-old female resident of the Cincinnati Address (“Minor Victim”), who was later forensically interviewed at a local center for abused children.

9. Individual-1 was shown photographs from the Toy album. Individual-1 stated, in substance and in part, that (1) MARK BROOKBANK, the defendant, lived with them at the Cincinnati Address since approximately June of 2017; (2) BROOKBANK was the adult male in

the photographs from the Toy album; (3) Minor Victim was the girl in the photographs from the Toy album; (4) the photographs from the Toy album were taken in the kitchen and Minor Victim's bedroom; and (5) BROOKBANK has an Apple iPhone 7, and the internet service provider for the Cincinnati Address is Cincinnati Bell.

10. Individual-2 was shown photographs from the Toy album. Individual-2 stated, in substance and in part, that (1) the girl in the photographs from the Toy album was Minor Victim; and (2) the adult male in the photographs was BROOKBANK.

11. Individual-1 gave permission for us to look around Minor Victim's bedroom and the general areas of the house. I located what appear to be the clothing and blanket that appeared in some of the images in the Toy album.

12. On or about December 21, 2017, the Court of Common Pleas in Hamilton County issued a search warrant for the bedroom at the Cincinnati Address in which BROOKBANK resided. I and other law enforcement executed the search warrant. From that search, we found, among other things, the following: (1) the slippers and pants in the photographs from the Toy album; (2) a collection of child's underwear; and (3) a laptop computer and six thumb drives.

13. I performed a forensic preview of the thumb drives and found child pornography.

14. On or about December 22, 2017, I arrested BROOKBANK pursuant to a federal arrest warrant. When BROOKBANK was arrested, the Device was located on the car seat next to him, which was seized incident to the arrest.

15. Also on or about December 22, 2017, after waiving his rights under *Miranda*, BROOKBANK said, in substance and in part, that (1) he had been downloading and distributing child pornography for years; (2) he actively traded child pornography on the internet; (3) he used the Device to take the pictures of Minor Victim; and (4) he uploaded the photographs to the

internet.

16. On or about January 3, 2018, MARK BROOKBANK was indicted by a grand jury in the Southern District of Ohio on one count of attempted production of child pornography and one count of possession of child pornography. *See United States v. Mark Brookbank*, 18-CR-001.

**CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN
CHILD PORNOGRAPHY AND WHO HAVE A
SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN**

1. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who view and possess multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to

lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area, cellular phone, and electronic storage media. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the individual to view the collection, which is valued highly.

e. Based on my training and experience, I know that individuals are increasingly utilizing laptop computers, cellular telephones and tablet computers to do their computing. In my experience, I know that individuals involved in child pornography offenses often utilize both computer devices and their cellular telephones to obtain and store their child pornography files. Due to their portable nature, laptop computers, cellular telephones and tablet computers provide individuals easy access to their files.

f. I know, in my experience, that individuals involved in child exploitation offenses often save their child pornography files on multiple devices, and they sometimes print the

pictures in hard copy format. Such individuals do so both for easier access / viewing of the files and to back-up the files in the event that one computer device becomes damaged and broken. Similarly, these individuals often save contact information (i.e., email addresses and account names) for those with whom they communicate about child exploitation offenses in multiple locations.

g. In my experience, I know that due to the covert nature of the devices, individuals involved in child pornography offenses also utilize their cellular telephones and tablet computers to take photographs of children and produce child pornography. Based on my training and experience and examination of similar devices, I know that most cellular telephones and tablet computers have digital cameras capable of taking photos and video.

h. Again based on my training and experience and examination of similar devices, I know that many laptop computers, cellular telephones and tablet computers have the ability to connect to the Internet. Individuals involved in child pornography offenses often utilize their laptop computers, cellular telephones and tablet computers to access Internet websites, exchange email messages, and access social media accounts to search for, view, and download child pornography.

i. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors /collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

j. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

2. In my training and experience, MARK BROOKBANK exhibits the common characteristics described above of someone involved in the distribution, receipt, production, and possession of child pornography, as evidenced by the facts that are set forth in this Affidavit.

TECHNICAL TERMS

3. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special

sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

h. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

i. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

4. Based on my training, experience, and research, I know that the Device is a cellular telephone and that most modern cellular telephones have capabilities that allow them to serve as “a wireless telephone, digital camera, portable media player, GPS navigation device, and PDAs.” In my training and experience, examining data stored on the Device of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

5. Based on my knowledge, training, and experience, Affiant knows that electronic devices can store information for long periods of time. Similarly, things that have been viewed

via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

6. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

7. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

8. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

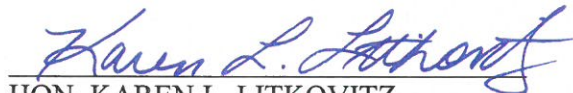
9. For these reasons, your Affiant submits that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B, which are evidence of a violations of Title 18, United States Code, Section 2251(a), and Title 18, United States Code, Section 2252(a)(4)(B).

Respectfully submitted,



Jason G. Kearns
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on April 16, 2018.



HON. KAREN L. LITKOVITZ
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched are the following electronic device, currently located at the Homeland Security Investigations office, 9875 Redhill Drive, Blue Ash, Ohio:

Apple iPhone cellular phone, marked Model A1661, FCC ID # BCG-E3087A, IC: 579C-E3087A (the "Device")

ATTACHMENT B

All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 2251(a) and 2252(a)(4)(B), (production and possession of child pornography), including but not limited to the following:

- a. Any visual depictions and records related to the production, possession, receipt, and distribution of child pornography;
- b. Any visual depictions of minors;
- c. Any Internet history indicative of searching for child pornography;
- d. Any Internet or cellular telephone communications (including email, social media, and online chat programs) with others in which child exploitation materials and offenses are discussed and/or traded, and any contact / identifying information for these individuals;
- e. Any Internet or cellular telephone communications (including email, social media, and online chat programs) with minors, and any contact / identifying information for these minors;
- f. Evidence of utilization of email accounts, social media accounts, online chat programs, and Peer-to-Peer file sharing programs, including any account / user names;
- g. Any information related to Internet Protocol (IP) addresses and Wi-Fi accounts accessed by the Device;
- h. Any GPS information on the Device;

- i. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
- j. Evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- k. Evidence of the lack of such malicious software;
- l. Evidence indicating how and when the Device was accessed or used to determine the chronological context of Device access, use, and events relating to crime under investigation and to the Device user;
- m. Evidence indicating the Device user's state of mind as it relates to the crime under investigation;
- n. Evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;
- o. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;
- p. Passwords, encryption keys, and other access devices that may be necessary to access the Device;
- q. Records of or information about the Device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

- r. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space.